Toward Safer Intimate Futures:
Recommendations for Tech Platforms to Reduce Image Based Sexual Abuse

Lucy Qin Brown University
Vaughn Hamilton Max Planck Institute for Software Systems
Yigit Aydinalp European Sex Workers Rights Alliance
Marin Scarlett European Sex Workers Rights Alliance
Sharon Wang University of Washington
Elissa M. Redmiles Max Planck Institute for Software Systems

Executive Summary

Sharing intimate images is common among adults for both recreational and commercial reasons. While sharing intimate images has many benefits, it can put people at risk of a form of technology-facilitated violence referred to as image-based sexual abuse (IBSA): the non-consensual, distribution or threat of distribution of intimate images.

We interviewed 52 European adults who create and share intimate images for recreational and/or commercial purposes to analyze their motivations for sharing intimate content, the technologies they employ, threats they face, and safety strategies they use to avoid non-consensual distribution of intimate images.

Storing and Sharing Intimate Images

• Participants used >40 technologies for creating, storing, or sharing intimate images, including messaging apps, social media platforms, dating apps, adult content platforms, and email.
• Technologies were chosen for reasons such as safety, convenience, popularity, recipient preference, profitability, and hospitability to use case.

Threat Models & Safety Strategies

• Four main NDII threats were identified: intentional sharing by recipients, platform or device hacks, device theft, and unintentional viewing (shoulder surfing).

• LGBTQ and sex working participants described concerns about NDII related to their identity and potential "outing" to friends, family, and coworkers.

• Participants incorporated protective strategies to reduce risk of NDII, including technological (e.g., watermarking, E2EE) and behavioral (e.g., removing identifying features, trust hierarchies).

Recommendations for Safer Futures

Broadly implement existing safety features

• None of the existing technologies offer all of the safety features participants used, and most offer only a few.

• We suggest a full suite of safety features to integrate into any platform on which image & video content can be stored or shared including enhanced options for screenshot & download management, content- and thread-level password protection, and sharing management.

Offer Visible & Preset Safety Settings

• Participants simultaneously use safety features, but doing so is cumbersome.

• Platforms should incorporate privacy presets based on intimate content sharing use cases such as an "intimate" picture or conversation mode.

Improve Usability and Transparency

• Digital fingerprinting may provide a way to track and identify non-consensual sharing, but further research is needed to resolve potential security/privacy risks.

• Existing tools need to be more transparent in how they implement fingerprinting technology.

Reallocate Responsibility to Platforms

• The burden of preventing NDII needs to be shared by platforms, not shouldered by those sharing intimate images alone.

• Technologies should prioritize features that favor individual autonomy, safety, and ease of use.

Table of Contents

Introduction & Background.....4

Choosing Technologies for Storing & Sharing Intimate Images.....5
Safety.....6
Convenience.....6
Interpersonal.....7
Commercial.....7

Safety Maze: Threat Models & Proactive Strategies for Safety.....8
Technological Strategies.....9
Behavioral Strategies.....11

Safer Futures: Recommendations for Reducing Image Based Sexual Abuse.....12
Recommendation #1: Implement Full Suite of Safety Features For Intimate Images.....12
Recommendation #2: Offer Visible & Preset Safety Settings for Intimate Interactions.....13
Recommendation #3: Improve Usability & Transparency for Advanced Protections.....13
Recommendation #4: Reallocate Responsibility from Individuals to Platforms.....14

Methodology.....15
Demographics.....15
Ethics, Impacts & Research Justice.....16

References.....17

Acknowledgements

This work was funded in part by the European Sex Workers Rights Alliance via a grant from the European AI & Society Fund, by the Max Planck Institute for Software Systems, by the Graduate Research Fellowship through the U.S. National Science Foundation, and by U.S. National Science Foundation Award # 2206950.

Contributions

ESWA proposed the project; LQ, VH, SW and EMR developed the interview protocol; LQ VH SW EMR and ESWA engaged in recruitment and conducted interviews; LQ VH SW analyzed the interviews; LQ VH SW EMR drafted the briefing paper; ESWA revised the briefing paper.

Introduction & Background

Sharing intimate images[1] is a common practice among adults. A recent survey in Norway found that 29.3% of the 4,000 adult respondents to their survey had sent a nude image [1]. Similarly, a survey in Germany found that 25% of their adult participants had sent an intimate image [2]. Sharing intimate images can improve relationship intimacy [3]–[6], provide employment, and be an expression of body positivity [2]. However, various forms of technology-facilitated violence have also increased such as the non-consensual creation, distribution, or threat of distribution of intimate images, which are collectively referred to as image-based sexual abuse (IBSA) [7]. In this work, we focus on addressing the non-consensual distribution of intimate images (NDII).

Motivations for Sharing Intimate Content:

"I have long term clients. And it kind of became part of the thing that I do for them for the same price. Like instead of seeing each other I send them some videos because we cannot see each other." **P44**

"So, I was on Mastodon...early [in] my transition, I had the need to just share so pictures [to] feel sexier. And so, I created an account, especially for that, that is networked with mostly other trans women that also have these accounts for the exact same purpose." **P26**

"I have like a craving for praise. And so that motivates me to share, to share my body with people who might enjoy it. So usually, I just check people, like, I'm not really picky. I just look for people [on Twitter] who are interested in seeing those kind of pictures." **P3**

To understand the technology landscape in which NDII occurs, we conducted an empirical study in which we interviewed 52 creators and sharers of intimate images for recreation (sexters) and commercial (sex workers) purposes (see Methodology for further detail). Our results shed light on the use cases of intimate image sharing, the technologies used in the creation, storage, and sharing of intimate imagery, and the threat models & defensive strategies people use in an effort to prevent abuse. We conclude with four recommendations for a safer intimate digital future.

As illustrated by the quotes in the sidebar, the use cases for sharing intimate images widely vary. Thus, it is important to understand how technology is used across these different contexts in order to identify points for intervention. People may create intimate images to sell and/or to share with an intimate partner, a stranger they met online, or a group of people (known or unknown).

People typically send intimate images with the expectation that they will not be shared without their consent [5]. Thus, they have significant concerns about non-consensual sharing, unwanted attention or sexual contact, blackmail, vulnerabilities or privacy issues with platforms used for storing or sharing intimate images,

[1] We define intimate images as photos or videos in which an individual is nude, semi-nude, or has intimate body parts visible and/or images or videos shared with the intention of causing arousal.

and/or the escalation of harassment [4]. When sharing intimate images, online guides suggest practices like using end-to-end encrypted platforms, disabling automatic backups on personal devices used to capture images, using self-deleting messages when appropriate, or removing identifying details in pictures. Yet, not all such strategies are compatible with every sharing use case and, even with the use of mitigation strategies, intimate images are often shared without consent.

Research estimates that up to 1 in 5 people have been threatened with or experienced NDII [8], [9]. According to organizations that support victim-survivors[2] of intimate partner violence, this abuse is increasing in volume [12], [13]. NDII disproportionately harms marginalized groups: young women [12], [14], [15], LGBTQIA people [12], [16], migrants [16], and victim-survivors of intimate partner violence [17]. NDII causes significant harm to people's mental health and may threaten their physical safety, reputation, or job security [18]; research has shown that victim-survivors of NDII may experience a feeling of loss of control and mental health symptoms similar to other forms of sexual violence that result in clinical diagnoses of anxiety, depression, and/or post-traumatic stress disorder [19], [20]. For sex workers, NDII also results in financial harm when commercial content is stolen, on top of fears of outing and future repercussions (e.g., in a different career) [21], [22].

A common form of resolution individuals may look toward is the removal of their non-consensually shared content from platforms, but there are many barriers to doing so. Perpetrators may purposely upload content to platforms that are specifically used for non-consensually shared intimate images that require individuals to pay a large sum of money for content removal [14]. Intimate images may also be shared in discreet or ephemeral online forums/groups that evade easy detection, such as on Telegram groups that are frequently deleted [23], [24]. Individuals who are able to identify and locate intimate images that have been shared without their consent may have difficulty getting that content removed from platforms due to their unresponsiveness or arduous reporting process [5].

Although more laws are being introduced globally to broadly address various forms of IBSA, there are limitations to seeking legal justice. There may still be language in legal discourse that subtly blames victims or shames victim-survivors. Particularly for women, the framing of legal cases may overemphasize the protecting of the survivor's virtue and reputation, even labeling victim-survivors as "ruined," rather than focusing on the violation of trust, privacy, and personal autonomy [25]. Further, stigma and poorly worded or outright discriminatory laws

[2]We chose to use the terminology victim-survivor to capture the range of ways in which people who have experienced IBSA may identify [10][11].

regarding sex work [26] for those selling intimate images and the resultant need for anonymity makes legal justice particularly inaccessible for those who experience NDII in regards to content they sell [22]. For example, in the United States, sex workers must provide a legal name and address in order to leverage copyright laws, which may then also be visible to the very people who committed the NDII [21]. In addition, litigation is expensive and victim-survivors may not know who the perpetrator is, or, if they do, they may fear retaliation.

As a result of these limitations in mitigating the non-consensual distribution of intimate images after it occurs, our report focuses on proactive mitigations. In the remainder of this report, we detail the technologies used to create, store, and share intimate images; the proactive strategies used by intimate image creators to protect themselves from abuse; and participants' requests for safer future technologies that could prevent NDII from the outset.

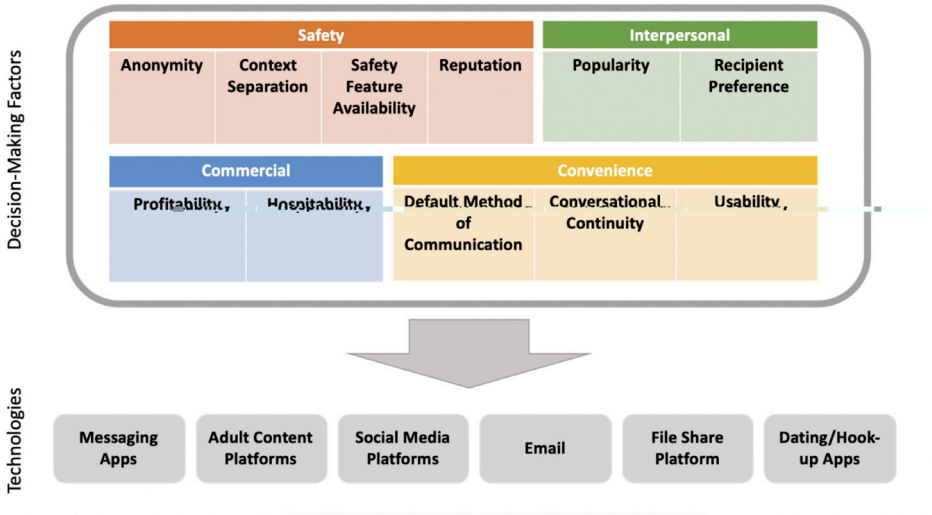
Choosing Technologies for Storing & Sharing Intimate Images

If a technology can be used for creating, storing, or sharing intimate images, it will be. Our participants used more than 40 different technologies. As one participant (P12) summarized:

> *"I've got like Telegram, I've got Signal, I've got WhatsApp, I've got Kik, you know, like, you name it, I've got it.*
> *And that's the general way that I send [intimate images].*
> *Although, you know, occasionally, if there's something really large, then that, you know, requires drop boxes and that sort of thing. And I'll do that."*

Broadly, participants used messaging applications, social media platforms, dating applications, adult content platforms, file share platforms, and email to share intimate images. They decided which applications to use based on a variety of factors including safety, convenience, interpersonal, and, when applicable, commercial considerations. Although we discuss different factors below in isolation, the reasons participants use a specific platform are multi-faceted. For example, P17 explains their decision process:

> *"Encryption and security would be probably the number one consideration. Number two is convenience. Once I know it's kind of safe, it's whatever is convenient for me to get the picture out to where it needs to be."*



Safety

Participants chose some sharing technologies because they offered anonymity. Anonymity can be particularly critical for sex workers. As P37 explains, *"I need a phone number for [Viber or WhatsApp] that is separate from the one that they use in my personal life and it's not really easy. Actually, you cannot obtain such a telephone number without giving your personal information like your name, your surname and such stuff in Greece. In Greece, doing escorting is illegal."*

Participants also selected particular apps to be exclusively used for intimate images for context separation. P15 explains that they chose Messenger for sending intimate content because they *"have WhatsApp for my work associates and everything so Messenger was only with close friends…I didn't want to mix like apps that I was using outside of principle."*

Participants also sought safety feature availability: they looked for options for protecting their content (see Safety Maze). Finally, participants relied on the reputation of a platform or service to assess whether it was safe to use for sharing intimate images. People determined a platform's reputation through the impressions of those close to them, news articles (e.g., about data breaches, data sharing), and platforms' level of transparency about data protections and use.

Convenience

Security was not the only – or in some cases, primary – motivator for selecting technologies to share intimate images. Almost half of the participants chose a particular sharing technology because it was their

default method of communication with the recipient. Given that many participants shared intimate images in the middle of a conversation, and in some cases spontaneously, they wanted to maintain the continuity of the conversation by using their default method of communication. As P43 described, *"...it's like at the heat of the moment, while you're talking and then you want to send the photo, to do another process to make it longer just doesn't make any sense."*

Several participants also described picking a sharing technology based on usability. For example, P18 found that web support was a feature that made WhatsApp more usable: *"I can use Web WhatsApp to type on my computer because I really hate being on my phone."* P37 wanted the option to not view porn during the process of uploading and checking the performance of the content they uploaded to adult content platforms, *"in order to check my statistics, I sometimes have to go through pages that show me porn... [the user interface is] a bit too busy, and I don't find it usable and I don't even like it."*

Interpersonal

Participants also chose sharing technologies because of their popularity or their recipient's preference. Those who shared in groups wanted to ensure that they used a platform with an active user base interested in consuming their content. People were also willing to accommodate the preference of the person with whom they were sharing. For example P12 explained that they use several sharing technologies in order to accommodate the preferences of their recipient, especially if *"those preferences surround privacy, or, you know, they feel really strongly about having limitations on things. I try to, like, be respectful of that."*

Commercial

Sex working participants also chose sharing technologies based on their profitability: those sharing content commercially sought platforms that were popular, offered flexibility in setting rates, and provided ease in payment processing. Finally, sex working participants also emphasized the importance of the platform's hospitability for sex work specifically. For example, P48 explained that they used a particular platform that was more complex to use *"not only because it's made by sex workers, but like, it's more like a gay, kinky, queer environment."*

Safety Maze: Threat Models & Proactive Strategies for Safety

Participants worried about four threats that might lead to NDII: intentional sharing of their intimate images by recipients, hacks of the platform or device on which they store or share images (either targeted attacks or software vulnerabilities), theft of the devices on which they stored content, and unintentional viewing of their content (e.g., shoulder surfing while in public).

Regardless of the mechanism through which they feared their content would be shared, participants described concern about the repercussions of NDII given their identity. For LGBTQ and sex working participants, the risk was magnified if they or their partner was not out, or their identity was a personal risk to them or the recipients of their images. P49 told us: *"I'm afraid that someone from my family would see that... It's the most stressful thing for me."*

Participants feared awkward or even dangerous situations with family, friends, their communities, and places of work and study. P18 hoped that if their images were shared that the focus would be on the person who shared them, but was realistic about how likely this would be:

> "What would happen if my colleagues were sent naked photos of me?
> I would like to think that it would be a non-issue, and instead, the focus will be on the person who was non-consensually sharing images of me.
> But unfortunately, there is a lot of victim blaming."

In an effort to proactively prevent NDII, participants reported using a kaleidoscope of technological and behavioral protective strategies. Some participants used these strategies all the time, while others changed what strategies to use based on their level of trust with a recipient and the context of their sharing (e.g., when in a country that criminalized their identity).

Technological Strategies

Some participants sought out sharing technologies that provided their preferred safety features while those who preferred to share intimate images within the context of their default messaging application used such features when available. When participants' preferred technological strategies were not offered by their platform of choice, some used third-party tools or manually enacted the desired functionality (e.g., mimicking the functionality of disappearing messages manually by periodically deleting content).

Technological strategies are not only used for technical protection: participants used strategies they perceived as insecure in order to implicitly communicate boundaries. For example, P2 explained that while *"disappearing messages are insecure by definition...if you send someone a disappearing message it's a clear, unambiguous sort of caption that says I would prefer if you didn't hold on to this."*

Hidden/locked folders enable users to move photos from the default view of a storage method (such as a smartphone gallery) into a designated folder and/or add password protection to specific folders on a device. Participants used such folders to protect their privacy when sharing a device and to protect against device theft and shoulder surfing (looking over someone's shoulder to see their device screen).

End-to-end encryption ensures that only a sender and their intended recipient(s) can view a message. This prevents a third-party that helps transport the image, such as a messaging platform, from being able to view it. However, once an end-to-end encrypted message has been delivered, it carries similar risks to unencrypted messages: the recipient can still store it to their device or share it. Despite this, some participants viewed messaging platforms that implemented end-to-end encryption as more trustworthy and/or more security-conscious.

Disappearing messages allow a sender to set a message expiration time after which a recipient can no longer view it. Expiration does not guarantee that a platform has deleted the content, nor does it prevent a recipient storing the content before expiration. While many used disappearing messages, others noted their limitations (e.g., they may incentivize recipients to store content).

Screenshot notifications notify the sender if the recipient screenshots the message. This does not prevent a recipient from circumventing the notification by taking a picture of the message with another device. Most participants found such notifications useful and one-fifth were more likely to use a platform that had them. However, they were aware that the feature could be circumvented and several emphasized the need for screenshot prevention, a feature offered by few platforms they used.

Watermarking is used to apply a visible (or invisible) signature to content. The watermark may potentially be used to identify the individual who created the content, depending on the watermark applied. Watermarks were more commonly used for commercial content and by recreational participants who used platforms that automatically watermarked their content.

Metadata removal is used to strip data about when or where an image/video was taken, which is often automatically added by a smartphone camera. Those who did metadata removal did so using third-party tools or manually, as none of the sharing technologies they used offered automated removal; others found it too cumbersome to do regularly.

General security hygiene such as enabling passwords on all their devices, using strong passwords on their devices and accounts, and enabling two-factor authentication for storage methods or accounts that could be susceptible to being hacked was used by many participants.

Though less commonly mentioned, participants also used features that enabled them to share masked content (e.g., recipients receive a blurred message and must click on the content to deblur it), remove content after it has been shared (e.g., unsend a message), and/or prevent the auto-downloading of images.

Behavioral Strategies

In conjunction with technological strategies, participants also employed behavioral strategies such as:

Removing and/or concealing identifying features from images, such as their face, unique features on body (i.e., birthmarks, tattoos), and/or backgrounds that may reveal their location. About half of our participants did this, either technologically using photo editing tools or by selectively framing their photos due to concern over reversibility and data privacy of third-party editing tools.

Setting explicit boundaries with recipients to establish whether and when intimate images can be stored and shared. Three quarters of participants engaged in such boundary setting. Some participants aimed to enforce these boundaries by reminding the recipient of the boundary or potential consequences of violating it (i.e., legal action).

Establishing trust hierarchies as a personal heuristic for deciding when and whether to share intimate images in the context of a relationship. Some participants only shared intimate images within the context of an established relationship while others differentiated the sensitivity of the content they share and the protective strategies they practiced based on the sharing relationship.

Vetting potential recipients through both formal and/or informal mechanisms. Formal mechanisms included checking IDs or receiving payment information while informal mechanisms include making intuition-based decisions (i.e., relying on a "sixth sense"), checking a recipient's social media profile, and/or video chatting prior to sharing.

Assuming content will be public and sharing content with the acceptance that once it has been sent, it is no longer within their control and might be shared more widely. This sometimes led to participants adopting additional safety strategies or to sharing content that they were more comfortable with being public.

Safer Futures: Recommendations for Reducing Image Based Sexual Abuse

Our participants shared with us their desires for safer digital futures, describing the features and implementations of those features that they felt would ensure a future without NDII. These recommendations are appropriate for a wide range of technologies – any that can be used to store and send intimate content – and thus should be considered by most if not all platforms when designing security protections.

Recommendation #1: Implement Full Suite of Safety Features For Intimate Images.

Participants shared that the technological features that would make them safer already existed, but all of the safety features they wanted to use were not simultaneously available on any of the platforms they used for storing and sharing images. Participants sought a balance between flexibility and availability; they wanted the features to be available but not required.

Participants specifically requested the integration of the following features:

- Watermarking for intimate images (such as that offered by OnlyFans [27]).
- Automatic metadata removal for intimate images (while third-party apps for automating removal exist, we are not aware of any sharing technologies with such a feature directly integrated).
- Sharing management options for intimate images: participants wanted both the ability to send disappearing/expiring content (such as that offered by Snapchat [28] and WhatsApp [29]) and the ability to recall messages after they had already been sent (e.g., once a relationship was terminated). As P6 explains, "the ability to retract would be nice, right? So, if you had a system where you can change access at any point in time, that would be helpful". This functionality exists in iMessage [30] and WhatsApp [31] although using those features requires the sender to find and action their original message; there is no present functionality to mark sensitive messages for later or periodic review.
- Password protection options for intimate images: password protection for individual images, folders, and conversations (such as that offered by WhatsApp [32]).
- Screenshot/download management options for intimate images: from notifications (such as those implemented by Snapchat [33]), to the ability to do mutual consent negotiation (not offered by any platforms, to our knowledge), to screenshot/download prevention (such as that implemented by Netflix [34], Grindr [35], and Confide [36]).

Recommendation #2: Offer Visible & Preset Safety Settings for Intimate Interactions

Participants use multiple features simultaneously to protect their content (e.g., automatic watermarking, disappearing messages, and screenshot prevention). People use different feature combinations based on context: their personal threat model and the interaction in which they are engaged. Manipulating each of the safety settings listed in Recommendation #1 for each piece of content or interaction is cumbersome. Thus, participants suggested offering a preset *"intimate picture mode"* (P30) or several modes with preset settings appropriate for different interactions with different levels of trust (e.g., relationship partners vs. new acquaintances or groups). This suggestion aligns with best practice from academic privacy literature ([37], [38]), which recommends privacy presets based on user contexts or personas.

Recommendation #3: Improve Usability & Transparency for Advanced Protections

Participants wanted the ability to track their content and proactively identify when it was shared non-consensually. There are existing methods that aim to offer this functionality, which we broadly refer to as "digital fingerprinting", that use characteristics of a piece of data to create a "fingerprint" that can be used to identify it (e.g., a hash, which distills content to a string of letters and numbers).[3] Fingerprints can then be used to compare images and videos to one another in order to find and identify the same (or similar) content more easily.

Only 3 of our 52 participants had heard of digital fingerprinting and none had used it. When we explained the term, participants expressed a mix of interest and skepticism. Some had reservations about how the security protection would work and concerns about what information the fingerprints themselves could reveal. These concerns are reasonable: academic research shows that savvy perpetrators may be able to glean information about the original image from a fingerprint they obtain and can edit images to evade detection [39].

While there are existing tools such as StopNCII.org, which allows people to create fingerprints and check their content against images held by partner organizations (i.e., Facebook, Instagram, TikTok, Bumble, OnlyFans), they lack transparency as to how they are implementing this technology. It is therefore difficult for users and security/privacy experts alike to fully assess any potential privacy risks.

[3]A type of digital fingerprinting used for image and video content is called perceptual hashing, which detects similar content, such as images that have been cropped or slightly modified.

Finally, a few participants noted that identifying the content alone would not be useful since barriers exist to removing non-consensually shared content on many platforms. This emphasizes the need for proactive mitigation strategies to be coupled with increased post-harm responsiveness by platforms.

Future research should further explore security and privacy risks of fingerprinting technologies, transparency mechanisms to accurately describe the fingerprinting risks and protections, design paradigms for integrating digital fingerprinting into platforms, and user concerns about such deployment. Our recommendation to further *investigate* the potential of fingerprinting functionality for NDII should not be taken as an endorsement of this technology as a whole, especially when applied in other contexts. Use of fingerprinting technology has also been proposed as a solution to other content moderation problems, causing valid privacy and censorship concerns [40][41].

Recommendation #4: Reallocate Responsibility from Individuals to Platforms

Throughout our interviews, participants repeatedly mentioned themes of personal responsibility. They acknowledged the risk "inherent" in sending intimate images, expressed fear of exposure and desire for greater control and autonomy over their intimate images.

Left to navigate abuse prevention on their own, participants have taken it upon themselves to shoulder the burden of preventing it (see Safety Maze). The volume and stringency of security behaviors that our participants engaged in extends beyond the standard level of responsibility any individual sharing online content should be reasonably expected to assume. Despite how much effort they put into security, participants critiqued themselves for not implementing enough behaviors to prevent abuse. At the same time, they expressed a matter-of-fact understanding that, ultimately, whether they were abused was out of their control once the intimate image was taken and/or sent.

We conceptualize this as a form of victim blaming enacted by technological design that communicates the belief that a victim of sexual violence is at least partially responsible for (preventing) the consequences. Victim blaming within the context of IBSA is prevalent: a survey in Australia found that 62% of participants believe 'If a person sends a nude or sexual image to someone else, then they are at least partly responsible if the image ends up online' [9] and the policies of many platforms perpetuate victim blaming messages [42].

To expect individuals who share intimate images to be responsible for where their images end up when there are technological features capable of preventing this outcome is unacceptable. To work toward a digital future without intimate image abuse, we need to reconsider how much personal responsibility individuals must assume when engaging in sending intimate images and how much of that responsibility can be reallocated or alleviated by implementing technological safety features. When possible, prioritize making technology that works in favor of individuals' autonomy, safety, and ease of use. Implement features that relieve burden from users. Individuals should not have to pick between avoiding abuse and engaging in recreation or labor.

Methodology

Over the course of August to November 2022, we conducted 52 semi-structured interviews with adults (over 18 years old) living in Europe[4] who had shared intimate images in the past year. Our participants consisted of 23 sex workers who produced their own digital content and 29 individuals who had shared intimate images for noncommercial purposes; 26 were victim-survivors of IBSA (13 sex workers, 13 recreational participants). Participants were recruited via social media, relevant community organizations, and personal contacts. Interviews were an average of 47 minutes long, and participants were compensated with 50€. Interviews were transcribed manually and then analyzed via qualitative open-coding.

Demographics

Participants reported that they resided in Belgium, England, France, Germany, Greece, Ireland, Latvia, North Macedonia, Norway, Poland, Portugal, Serbia, Spain, The Netherlands, and the United Kingdom. 34 of our participants identify as White (including 2 mixed race individuals), 18 do not (among these 18 participants, 15 chose to report their race: 3 Black, 3 Latina/Latino/Latinx, 2 mixed race, 2 Brown). 14 of our participants were cis or trans women, 20 were cis or trans men, 11 were non-binary, gender fluid, or another gender, and 7 chose not to report their gender. 38 were queer, asexual, bisexual, pansexual, gay, or lesbian; 11 were heterosexual; and 5 chose not to describe their sexual orientation. Our participants were highly educated: 38 had a Bachelor's degree or higher education, 14 did not.

[4]As defined by the WHO: https://www.who.int/countries.

Ethics, Impacts & Research Justice

Our procedures were approved by the University of Saarland Ethics Review Board. To ensure the security and confidentiality of participant data, we implemented various precautionary measures. For virtual interviews, we utilized encrypted platforms like paid Webex, which offers end-to-end encryption. To safeguard communication, we provided guidelines on setting up encrypted email addresses using ProtonMail, enabling interview organization and reminders. Additionally, we employed a scheduling system called Calendly, which didn't require participants to disclose personal information such as their names during the scheduling process. Participants were given the choice of anonymous Amazon gift cards or PayPal payments, which could be sent to their encrypted email addresses created following our instructions. Sex working participants were given the option to be interviewed by a current or former sex worker and, in addition to having sex working researchers on our research team, we also hired a sex worker to transcribe the interviews.

References

[1] B. Træen and I. L. Kvalem, "Gender Differences in Sending Nude Pictures and Videos Across Multiple Relationship Contexts in the Adult Norwegian Population," *Sex. Cult.*, Oct. 2022, doi: 10.1007/s12119-022-10028-0.

[2] T. Falconer, C. Quinn-Nilas, and R. Milhausen, "Body image self-consciousness, sexting, and sexual satisfaction among midlife Canadians," *Can. J. Hum. Sex.*, vol. 31, no. 1, pp. 46–63, Apr. 2022, doi: 10.3138/cjhs.2021-0027.

[3] W. G. Macdowall et al., "Sexting among British adults: a qualitative analysis of sexting as emotion work governed by 'feeling rules,'" *Cult. Health Sex.*, pp. 1–16, Jun. 2022, doi: 10.1080/13691058.2022.2080866.

[4] Christine Geeng, Jevan Huston, and Franziska Roesner, "Usable Sexurity: Studying People's Concerns and Strategies When Sexting," in *The Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, USENIX Association, 2020.

[5] A. E. Waldman, "Law, Privacy, and Online Dating: 'Revenge Porn' in Gay Online Communities," *Law Soc. Inq.*, vol. 44, no. 04, pp. 987–1018, Nov. 2019, doi: 10.1017/lsi.2018.29.

[6] R. Amundsen, "Hetero-sexting as mediated intimacy work: 'Putting something on the line,'" *New Media Soc.*, vol. 24, no. 1, pp. 122–137, Jan. 2022, doi: 10.1177/1461444820962452.

[7] N. Henry, C. McGlynn, A. Flynn, K. Johnson, A. Powell, and A. J. Scott, *Image-based sexual abuse: a study on the causes and consequences of non-consensual nude or sexual imagery.* Abingdon, Oxon: Routledge, 2022.

[8] Asia Eaton, Holly Jacobs, and Yanet Ruvalcaba, "2017 Nationwide Online Study of Nonconsensual Porn Victiization and Perpetration," Cyber Civil Rights Initiative. [Online]. Available: https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

[9] Nicola Henry, Anastasia Powell, and Asher Flynn, "Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse," RMIT University, 2017. [Online]. Available: https://research.monash.edu/en/publications/not-just-revenge-pornography-australians-experiences-of-image-bas

[10] J. Williamson and K. Serna, "Reconsidering Forced Labels: Outcomes of Sexual Assault Survivors Versus Victims (and Those Who Choose Neither)," *Violence Women*, vol. 24, no. 6, pp. 668–683, May 2018, doi: 10.1177/1077801217711268.

[11] Sexual Assault Kit Initiative, "Victim or Survivor: Terminology from Investigation Through Prosecution," RTI International. Accessed: Jul. 14, 2023. [Online]. Available: https://www.sakitta.org/toolkit/index.cfm?fuseaction=tool&tool=80

[12] Amanda Lenhart, Michelle Ybarra, and Myeshia Price-Feeney, "Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of 'Revenge Porn,'" Data & Society Research Institute, Dec. 2016.

[13] Zara Ward, "Revenge Porn Helpline Report 2022," Revenge Porn Helpline, 2022. [Online]. Available: https://swgfl.org.uk/research/revenge-porn-helpline-2022-report/

[14] A. A. Eaton, S. Noori, A. Bonomi, D. P. Stephens, and T. L. Gillum, "Nonconsensual Porn as a Form of Intimate Partner Violence: Using the Power and Control Wheel to Understand Nonconsensual Porn Perpetration in Intimate Relationships," *Trauma Violence Abuse*, vol. 22, no. 5, pp. 1140–1154, Dec. 2021, doi: 10.1177/1524838020906533.

[15] T. Mckinlay and T. Lavis, "Why did she send it in the first place? Victim blame in the context of 'revenge porn,'" *Psychiatry Psychol. Law*, vol. 27, no. 3, pp. 386–396, May 2020, doi: 10.1080/13218719.2020.1734977.

[16] L. Vitis, "Private, Hidden and Obscured: Image-Based Sexual Abuse in Singapore," *Asian J. Criminol.*, vol. 15, no. 1, pp. 25–43, Mar. 2020, doi: 10.1007/s11417-019-09293-0.

[17] C. McGlynn, E. Rackley, and R. Houghton, "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse," *Fem. Leg. Stud.*, vol. 25, no. 1, pp. 25–46, Apr. 2017, doi: 10.1007/s10691-017-9343-2.

[18] T. Kirchengast and T. Crofts, "The legal and policy contexts of 'revenge porn' criminalisation: the need for multiple approaches," *Oxf. Univ. Commonw. Law J.*, vol. 19, no. 1, pp. 1–29, Jan. 2019, doi: 10.1080/14729342.2019.1580518.

[19] S. Bates, "Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors," *Fem. Criminol.*, vol. 12, no. 1, pp. 22–42, Jan. 2017, doi: 10.1177/1557085116654565.

[20] A. A. Eaton and C. McGlynn, "The Psychology of Nonconsensual Porn: Understanding and Addressing a Growing Form of Sexual Violence," *Policy Insights Behav. Brain Sci.*, vol. 7, no. 2, pp. 190–197, Oct. 2020, doi: 10.1177/2372732220941534.

[21] Vaughn Hamilton, Hanna Barakat, and Elissa Redmiles, "Risk, Resilience and Reward: Impacts of Shifting to Digital Sex Work," in *The Proceedings of the 25th ACM Conference on Computer-Supported Cooperative Work And Social Computing*, Association for Computing Machinery, Nov. 2022.

[22] C. Barwulor, A. McDonald, E. Hargittai, and E. M. Redmiles, "'Disadvantaged in the American-dominated Internet': Sex, Work, and Technology," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan: ACM, May 2021, pp. 1–16. doi: 10.1145/3411764.3445378.

[23] N. Henry and A. Flynn, "Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support," *Violence Women*, vol. 25, no. 16, pp. 1932–1955, Dec. 2019, doi: 10.1177/1077801219863881.

[24] S. Semenzin and L. Bainotti, "The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities," *Soc. Media Soc.*, vol. 6, no. 4, p. 205630512098445, Oct. 2020, doi: 10.1177/2056305120984453.

[25] A. Dodge, "'Try Not to be Embarrassed': A Sex Positive Analysis of Nonconsensual Pornography Case Law," *Fem. Leg. Stud.*, vol. 29, no. 1, pp. 23–41, Apr. 2021, doi: 10.1007/s10691-021-09452-8.

[26] European Sex Workers' Rights Alliance (ESWA), "The Impact of Online Censorship and Digital Discrimination on Sex Workers," Feb. 2022. [Online]. Available: https://www.eswalliance.org/the_impact_of_online_censorship_and_digital_discrimination_on_sex_workers

[27] OnlyFans, "OnlyFans Watermark," *Community Guidelines*, 2023. https://onlyfans.com/help/3/24/100 (accessed Jun. 24, 2023).

[28] Snapchat, "When does Snapchat delete Snaps and Chats?," *Snapchat Support*. https://help.snapchat.com/hc/en-us/articles/7012334940948-When-does-Snapchat-delete-Snaps-and-Chats-#:~:text=Snapchat%20servers%20are%20set%20to,keep%20any%20reactions%20to%20it. (accessed Jun. 24, 2023).

[29] WhatsApp, "About disappearing messages," *Help Center*, 2023. https://faq.whatsapp.com/673193694148537 (accessed Jun. 24, 2023).

[30] Apple, "Unsend and edit messages on iPhone," *iPhone User Guide*, 2023. https://support.apple.com/guide/iphone/unsend-and-edit-messages-iphe67195653/ios (accessed Jun. 24, 2023).

[31] WhatsApp, "How to delete messages," *Help Center*, 2023. https://faq.whatsapp.com/1370476507114859/?cms_platform=web (accessed Jun. 24, 2023).

[32] WhatsApp, "How to turn on chat lock," *Help Center*, Jun. 24, 2023. https://faq.whatsapp.com/764072925284841/?cms_platform=web

[33] Steven John, "'Does Snapchat notify users when you take screenshots?': Here's what you need to know," *Business Insider*, Oct. 28, 2019. Accessed: Jun. 24, 2023. [Online]. Available: https://www.businessinsider.com/guides/tech/does-snapchat-notify-screenshots

[34] Gavia Baker-Whitelaw, "Why you can't take a screenshot of a TV show or movie on your computer," Dec. 22, 2022. Accessed: Jun. 24, 2023. [Online]. Available: https://www.dailydot.com/unclick/netflix-block-screenshots-drm/

[35] Grindr, "Albums", *Help Center*. https://help.grindr.com/hc/en-us/articles/4414580688787-Albums#h_01FTRQMC7YBBR9D9EV5FBZX20A (accessed Jun. 24, 2023).

[36] Confide, "Your Confidential Messenger," 2023. https://getconfide.com/#:~:text=Confide%20prevents%20screenshots%20with%20our,name%20is%20not%20simultaneously%20visible. (accessed Jun. 24, 2023).

[37] B. P. Knijnenburg, "Privacy? I Can't Even! Making a Case for User-Tailored Privacy," *IEEE Secur. Priv.*, vol. 15, no. 4, pp. 62–67, 2017, doi: 10.1109/MSP.2017.3151331.

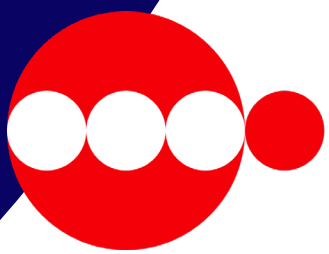
[38] P. Wisniewski, A. K. M. N. Islam, B. P. Knijnenburg, and S. Patil, "Give Social Network Users the Privacy They Want," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, Vancouver BC Canada: ACM, Feb. 2015, pp. 1427–1441. doi: 10.1145/2675133.2675256.

[39] Sarah Scheffler and Jonathan Mayer, "SoK: Content Moderation for End-to-End Encryption," presented at the Privacy Enhancing Technologies Symposium, Lausanne, Switzerland, Jul. 2023.

[40] Carmela Troncoso and Bart Preneel, "Commissioner Johannson's response to scientists' online privacy concerns goes after straw men," *Euronews*, Jul. 17, 2023. [Online]. Available: https://www.euronews.com/2023/07/17/commissioner-johannsons-response-to-scientists-online-privacy-concerns-goes-after-straw-me?utm_source=Twitter&utm_medium=Social

[41] Carmela Troncoso et al., "Joint statement of scientists and researchers on EU's proposed Child Sexual Abuse Regulation: 4 July 2023." Jul. 03, 2023.

[42] J. Bailey, A. Flynn, and N. Henry, Eds., *The Emerald international handbook of technology-facilitated violence and abuse*, First edition. in Emerald studies in digital crime, technology and social harms. Bingley: Emerald Publishing, 2021.



european
sex workers
rights
alliance

BROWN

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS

European
Artificial Intelligence
& Society Fund